



# **CERT Resiliency Engineering Framework**

**David White**

**01 March 2007**



Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>01 MAR 2007</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2007 to 00-00-2007</b>	
4. TITLE AND SUBTITLE <b>CERT Resiliency Engineering Framework</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Carnegie Mellon University ,Software Engineering Institute (SEI),Pittsburgh,PA,15213</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>34</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

# Software Engineering Institute

---

Established 1984

Federally Funded R&D Center (FFRDC)

College-level unit of Carnegie Mellon University

Five technical programs help organizations improve software-intensive systems

Widely-known “brands”

- CERT Coordination Center
- Capability Maturity Model Integration (CMMI)



# Agenda

---

**Context and problem**

**Resiliency Engineering**

**Process Improvement**

**The CERT Resiliency Engineering Framework**

**Future Plans and Summary**

# Today's operational environment

---

No operational boundaries

Increasing regulation

Pervasive & rapidly  
changing technology

Criticality of data and  
information

Dynamic & expanding risks

Distributed workforce

Fewer resources, more  
demands

Heightened threat level and  
increasing uncertainty

Dependency on third-parties

Shorter-lived skills

***A new environment in which business continuity  
& security must be increasingly effective & efficient***

# Operational risk management problems

---

Poor planning and execution

Poorly defined and measured goals

No asset management function

Reactive (not strategic) funding model

Seen as a technical function or responsibility

Compartmentalization of security and continuity activities

Searching for magic bullet: CobiT, ITIL, ISO17799, NFP1600

Business units not involved

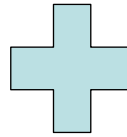
***Many organizations are struggling with operational risk management***

# Our approach

---

## **Resiliency Engineering**

An integrated approach to protecting & sustaining critical business services



## **Process Improvement**

A model-based approach to maturing enterprise capabilities



## **CERT Resiliency Engineering Framework**

A process improvement model for resiliency engineering

# Top benefits of approach

---

## **Greater efficiency of resilience activities**

- Optimized resource allocation
- Appropriate and strategic investment

## **Objective benchmarking of resilience capabilities**

- For internal improvement
- To evaluate third parties

## **Improved operational risk management**

- Measured processes lead to measured improvement
- Better risk management yields market rewards





# Resiliency Engineering:

*An integrated approach to protecting & sustaining critical business services*

# Resiliency engineering defined

---

The process by which an organization designs, develops, implements, and manages the protection and sustainability of business-critical services, related business processes, and associated assets such as people, information, technology, and facilities

“Requirements-driven security and business continuity”

# Resiliency engineering body of knowledge

---

Based on

- Affinity analysis of 750 best practices in security, business continuity, and IT operations
- Collaboration with business continuity experts from numerous US financial institutions
- Security expertise in CERT

Developed, collected, and codified over past two+ years

Forms the basis of our continuing work

# Operational risk and resiliency

---

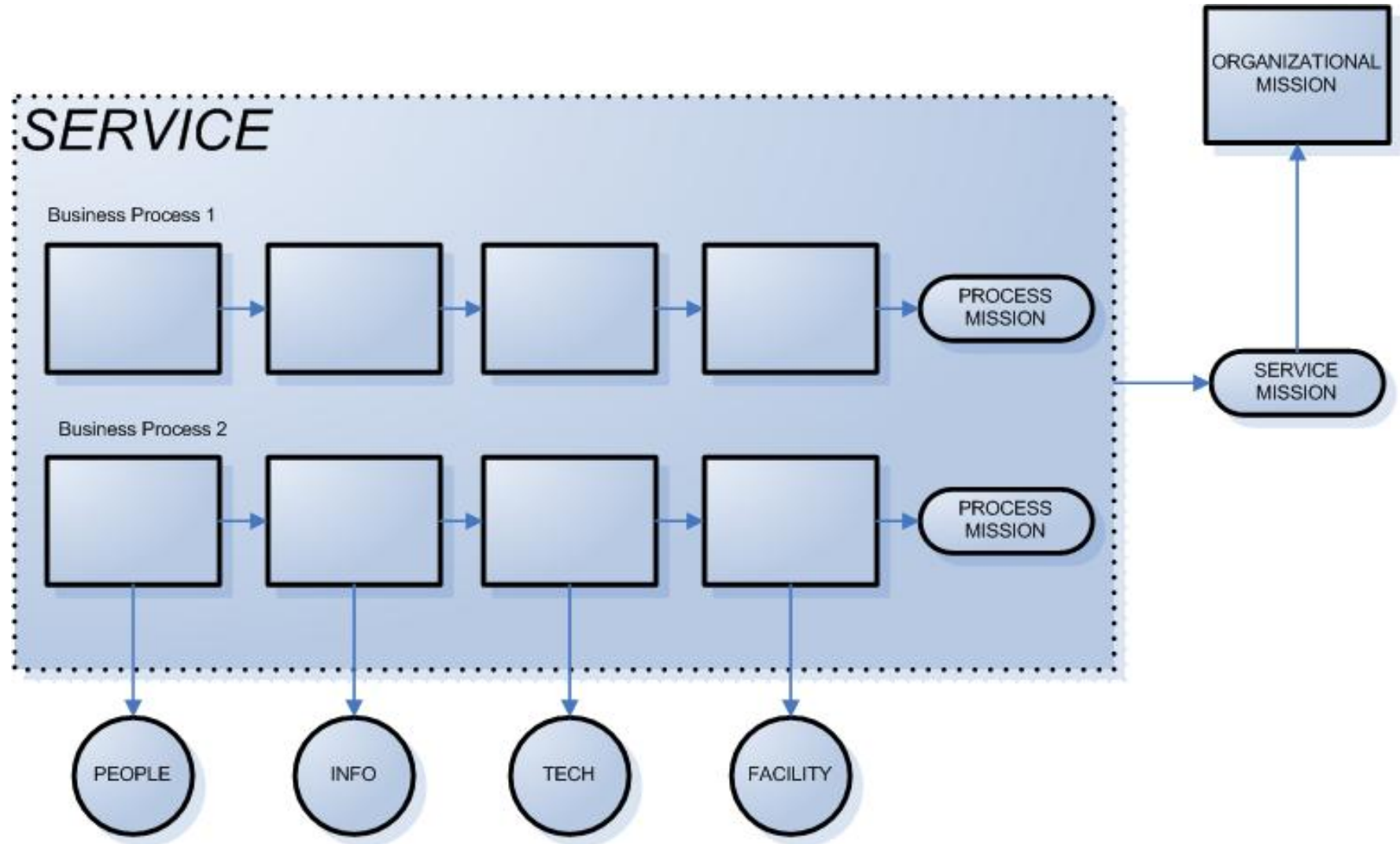
Operational risk is from

- Failed internal processes
- Inadvertent or deliberate actions of people
- Problems with systems and technology
- External events

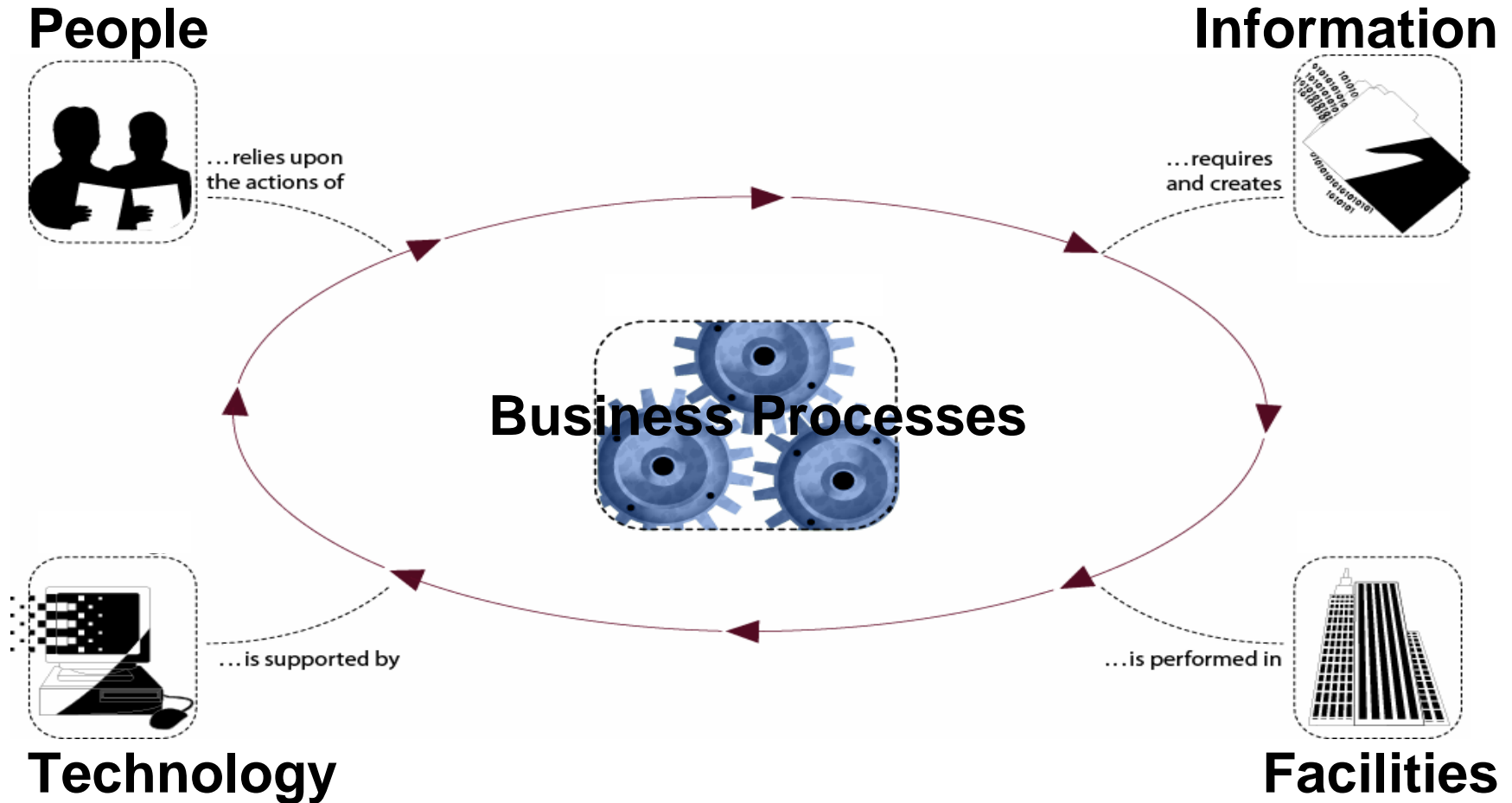


Operational resiliency is the ability to sustain the mission despite these risks

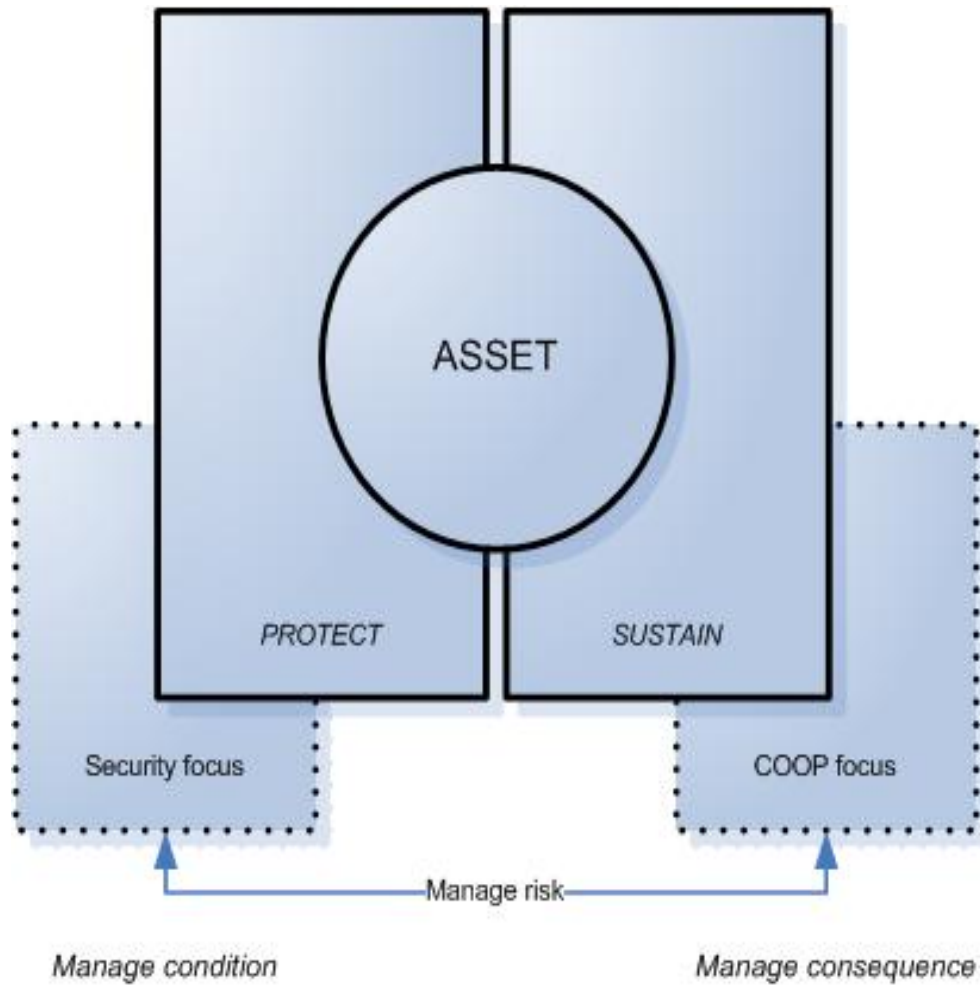
# A mission focus



# Dependence on four critical asset types



# Asset focus




Resiliency emerges from effectively coordinating and managing the conditions and consequences of risk

# Achieving resiliency

---

## Shift the paradigm

- Technical problem
  - Owned by IT
  - Expense-driven
  - Practice-centric
  - Security and BCDR
- 
- Business problem
  - Owned by organization
  - Investment-driven
  - Process-centric
  - Enterprise resiliency

Approach resiliency as a definable, manageable, improve-able, enterprise-wide process





# Process Improvement:

*A model-based approach to maturing enterprise capabilities*

# Process improvement defined

---

“A program of activities designed to improve the performance and maturity of the organization’s processes, and the results of such a program.”

Provides the basis for managing, sustaining, and improving the resiliency process over time

Distinguishes organizations that have good resiliency practices at one point in time from those who can be counted on to have good, ongoing resiliency practices

# How does process differ from practice?

---

## Process

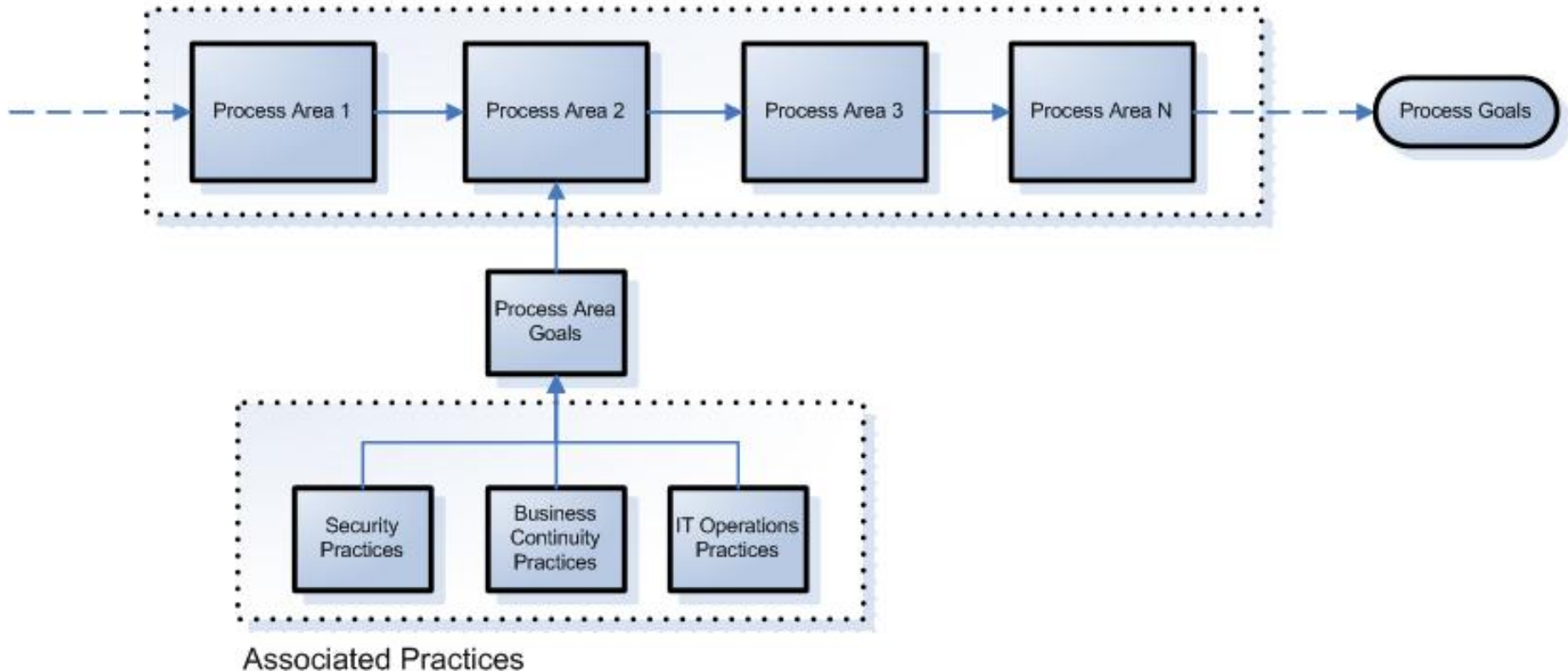
- Describes the “what”
- Based on process goals
- Manage process to requirements
- Select practices based on process goals
- Can be defined, communicated, measured, and controlled
- Long-lived

## Practice

- Prescribes the “how”
- No practice goals
- Tends toward “set and forget” mentality
- Reinforces domain-driven approach
- One size does not fit all
- Regulatory vehicle
- Short-lived

# Relationship between process and practice

## Enterprise Security and Resiliency Process



# Embracing process improvement

---

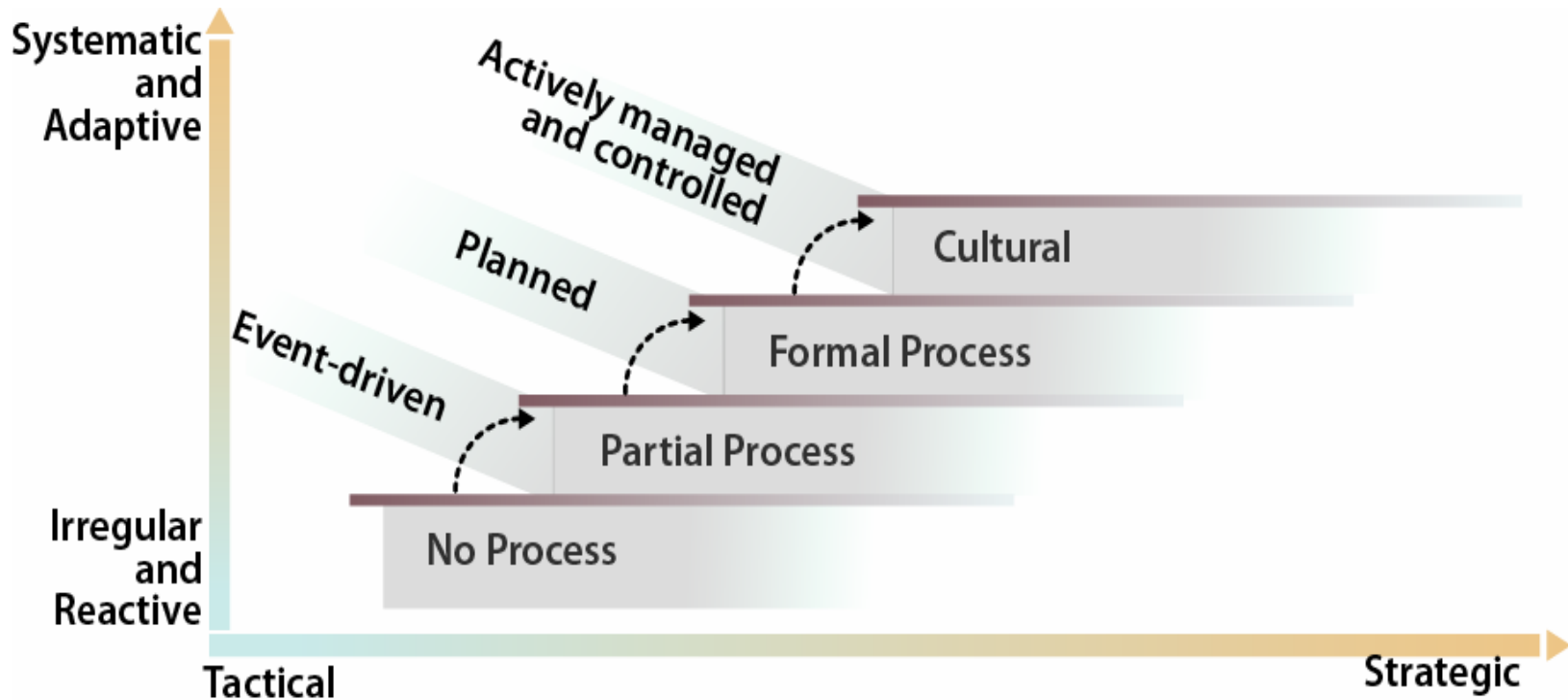
Improvement in meeting resiliency goals is dependent on the active management of the process

Process maturity increases capability for meeting goals and sustaining the process

“Are we resilient?” or “Are we secure?” is answered in the context of goal achievement rather than what hasn’t happened

Facilitates meaningful, purposeful selection and implementation of practices

# Process maturity shifts the paradigm



# Process improvement model

---

## Model or framework provides

- A common basis of comparison for planning and benchmarking process improvement
- Defined catalogue of capabilities to guide mastery in a particular domain
- Guidelines and goals for managing, sustaining, and maturing the processes that instantiate the organization's capabilities



# **CERT Resiliency Engineering Framework:**

*A process improvement model for  
resiliency engineering*



# The Resiliency Engineering Framework

---

A process framework for resiliency engineering

Defines basic capability areas and provides guidelines for security and business continuity process improvement

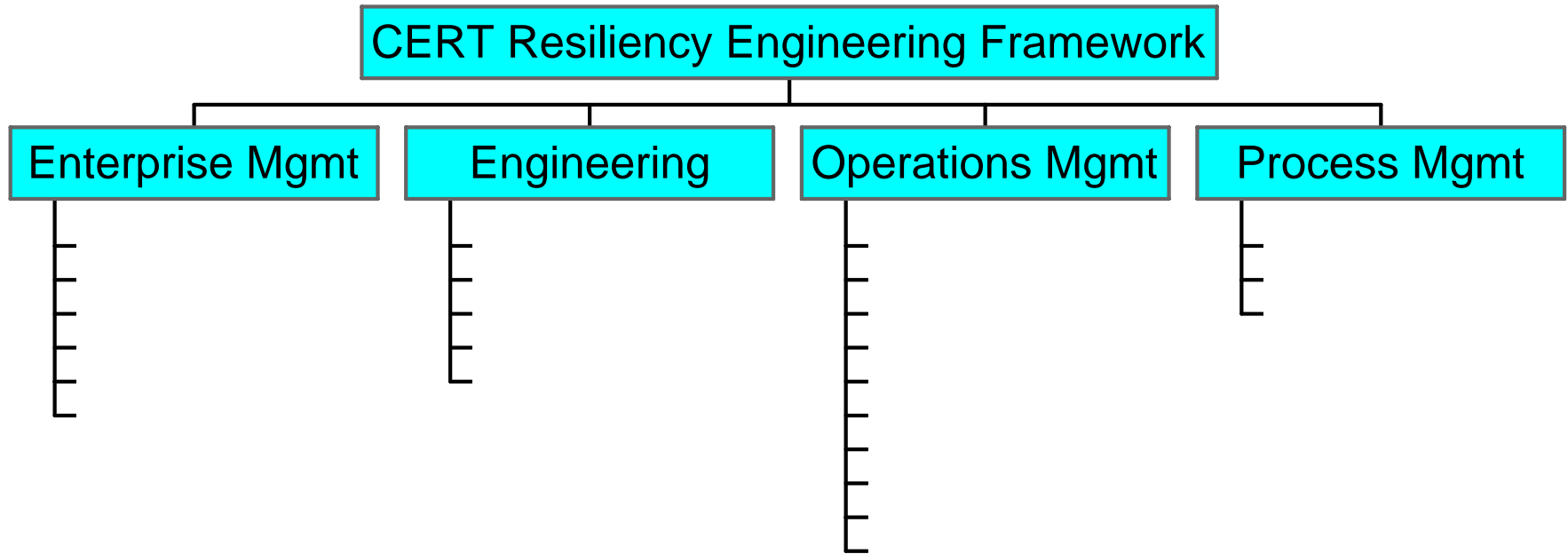
Captures vital linkages between security, business continuity, and IT operations

Addresses operational risk management through process management

Establishes a capability benchmark

# Framework architecture

---



24 capability areas

Focused on resiliency of people, information, technology, and facilities in the context of services and business objectives

# Using the framework

---

Benchmark current level of capability

Set forward-looking capability goals and targets

Develop plans to close identified gaps

Build resiliency into important assets and architectures

Reduce reactionary activities; shift to directing and controlling activities

Align common practices with processes to achieve process goals

# Framework status

---

Currently in outline

Based on resiliency engineering body of knowledge

Version 1.0 to be published this year



## **Future Plans and Summary:** *ongoing work to mature and disseminate the framework*

# 2007 Plans

---

Continued collaboration with financial sector through FSTC

Complete and publish framework version 1.0

Explore process maturity concepts

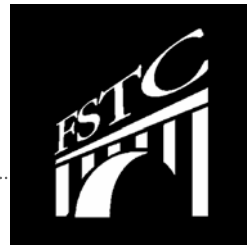
Pilot first assessment mechanism

Pilot early training curriculum

Conduct improvement pilots to validate model and approach

Expand REF community

# Financial Services Technology Consortium



Member-owned consortium of financial services-focused organizations

Explores new technologies to address industry business needs

## **FSTC project participants:**

AMD	Discover	KPMG	US Bank
Ameriprise	DRII	MasterCard	Wachovia
Bank of America	DRJ*	Marshall and Ilsley	Wells Fargo
Bank of Oklahoma	IBM	NY FRB*	
Capital Group	JPMorgan Chase	SunGard	
Citigroup	Key Bank	Trizec Properties	

\*observing participant

# Beyond 2007

---

Continue outreach and community building

Expand and refine REF product suite

- Model
- Publications
- Training
- Assessment/Appraisal
- Professional certifications for instructors and appraisers

Continued piloting and case study development

Support community adoption



# Summary

---

Today's environment calls for better operational risk management

Engineering and improving protection and sustainability processes will enhance operational resiliency

REF enables process improvement and benchmarking of operational resiliency capabilities

# How can you be involved?

---

Add your name to our mailing list to be informed when the framework and other project artifacts are available

Participate in a pilot assessment

Explore other forms of collaboration

# For more information

---



David W. White

Software Engineering Institute  
Carnegie Mellon University

[www.sei.cmu.edu](http://www.sei.cmu.edu)

[www.cert.org](http://www.cert.org)

dwhite@cert.org